

<insert letter> Detection & Response

Making Sense of it All

Friday, October 29, 2021

Introduction

Tim Lewis: NOC/SOC Manager at Mirazon

Introduction

Tim Lewis: NOC/SOC Manager at Mirazon

We'll be covering:

Introduction

Tim Lewis: NOC/SOC Manager at Mirazon

We'll be covering:

- The threat landscape and why we need "Detection & Response"

Introduction

Tim Lewis: NOC/SOC Manager at Mirazon

We'll be covering:

- The threat landscape and why we need "Detection & Response"
- What is "Detection & Response"

Introduction

Tim Lewis: NOC/SOC Manager at Mirazon

We'll be covering:

- The threat landscape and why we need "Detection & Response"
- What is "Detection & Response"
- The different kinds of "Detection & Response" offerings

Introduction

Tim Lewis: NOC/SOC Manager at Mirazon

We'll be covering:

- The threat landscape and why we need "Detection & Response"
- What is "Detection & Response"
- The different kinds of "Detection & Response" offerings
- What to look for in "Detection & Response"

The Threat Landscape

This is the scary slide

The Threat Landscape

This is the scary slide

- The first ransomware attack occurred in 1989 against AIDS researchers. 24% of data breaches occur in healthcare.

The Threat Landscape

This is the scary slide

- The first ransomware attack occurred in 1989 against AIDS researchers. 24% of data breaches occur in healthcare.
- The average cost of remediating ransomware is \$761,106.

The Threat Landscape

This is the scary slide

- The first ransomware attack occurred in 1989 against AIDS researchers. 24% of data breaches occur in healthcare.
- The average cost of remediating ransomware is \$761,106.
- In 2020, the average downtime due to ransomware was 19 days.

The Threat Landscape

This is the scary slide

- The first ransomware attack occurred in 1989 against AIDS researchers. 24% of data breaches occur in healthcare.
- The average cost of remediating ransomware is \$761,106.
- In 2020, the average downtime due to ransomware was 19 days.
- The average payment of targeted organizations is \$233,817.

The Threat Landscape

This is the scary slide

- The first ransomware attack occurred in 1989 against AIDS researchers. 24% of data breaches occur in healthcare.
- The average cost of remediating ransomware is \$761,106.
- In 2020, the average downtime due to ransomware was 19 days.
- The average payment of targeted organizations is \$233,817.



The Threat Landscape

But wait, there's more!

The Threat Landscape

But wait, there's more!

REvil member says gang targets organisations with cyber insurance for ransomware attacks

Dev Kundaliya

17 March 2021 • 2 min read

SHARE



Image: Alleged REvil member claims they target companies with cyber insurance

The Threat Landscape

But wait, there's more!

REvil member says gang targets organisations with cyber insurance for ransomware attacks

Dev Kundaliya

17 March 2021 • 2 min read

SHARE



Image: Alleged REvil member claims they target companies with cyber insurance

The Threat Landscape

But wait, I have anti-virus...

The Threat Landscape

But wait, I have anti-virus...

- More sophisticated attack strategies are outpacing anti-virus software.

The Threat Landscape

But wait, I have anti-virus...

- More sophisticated attack strategies are outpacing anti-virus software.
- The traditional anti-virus model relies too heavily on signatures.

The Threat Landscape

But wait, I have anti-virus...

- More sophisticated attack strategies are outpacing anti-virus software.
- The traditional anti-virus model relies too heavily on signatures.
- From Infosecurity Magazine:

Over two-thirds (70%) of all malware attacks involved evasive zero-day malware in Q2 of 2020, which is a 12% rise on the previous quarter, according to [WatchGuard Technologies](#) latest *Internet Security Report*.

Interestingly, the increase in this form of malware, which circumvents anti-virus signatures, has come as overall malware detections fell by 8% compared to Q1. WatchGuard attributes this reduction to the rise in remote working brought about by COVID-19, as less employees are operating behind corporate network perimeters.



The Threat Landscape

What is “Detection and Response?”

The Threat Landscape

What is “Detection and Response?”

- In short: a series of technologies/products that focus on detecting and investigating suspicious activity.

The Threat Landscape

What is “Detection and Response?”

- In short: a series of technologies/products that focus on detecting and investigating suspicious activity.
- Not necessarily a replacement for anti-virus, instead provides more data.

The Threat Landscape

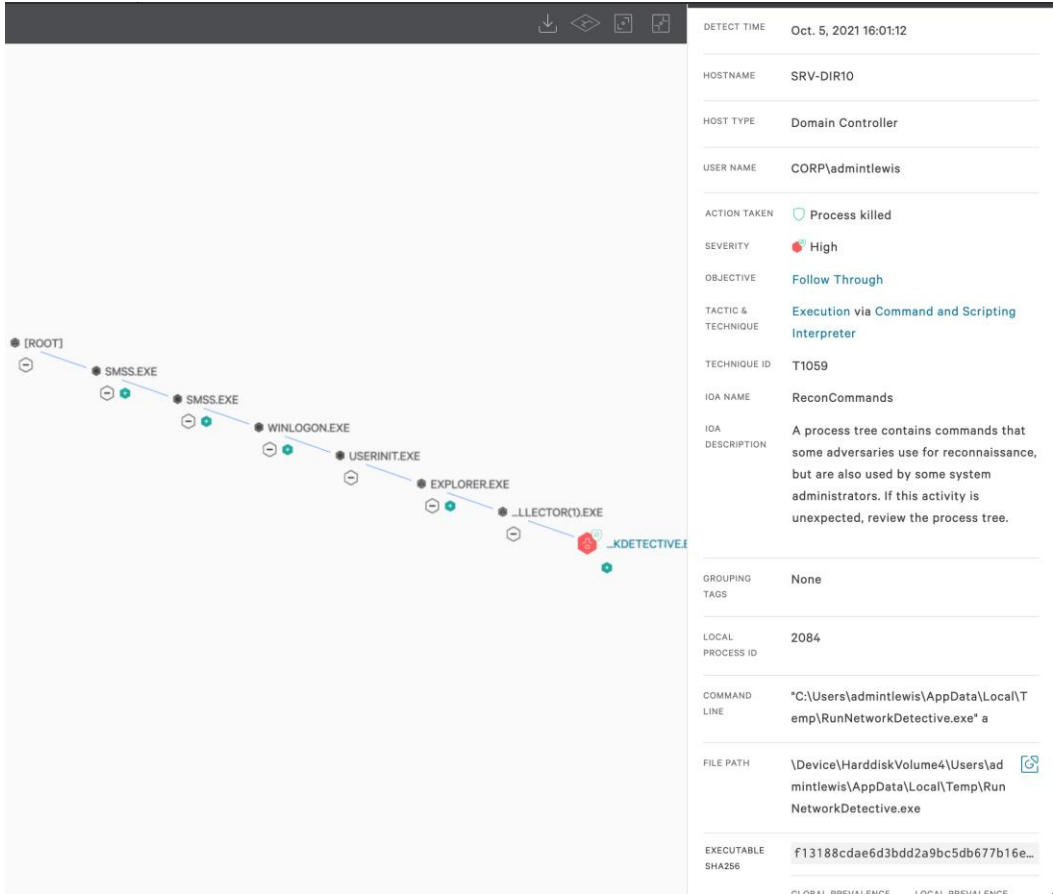
What is “Detection and Response?”

- In short: a series of technologies/products that focus on detecting and investigating suspicious activity.
- Not necessarily a replacement for anti-virus, instead provides more data.
- A lot more data...

The Threat Landscape

What is “Detection and Response?”

- A LOT more data



Oct. 5, 2021 14:26:35	Process start	winlogon.exe	winlogon.exe	Not running	3h 42m 35s	
Oct. 5, 2021 14:26:39	Process start	explorer.exe	C:\Windows\Explorer.EXE	Not running	3h 42m 30s	
Oct. 5, 2021 15:17:26	Process start	NetworkDetecti...	"C:\Users\adminitlewis\Downloads\NetworkDetectiveDataC...	Not running	7s	
	Event type	Hostname	Sensor version	IP address	Local IP address	
Oct. 5, 2021 15:17:27	Host	SRV VM33	6.29.14304.0	74.142.71.2	169.254.1.161	
Oct. 5, 2021 15:17:27	Host	SRV DIR10	6.29.14304.0	74.142.71.2	10.0.99.151	
Oct. 5, 2021 15:17:27	Host	SRV DIR11	6.29.14304.0	74.142.71.152	10.0.99.152	
Oct. 5, 2021 15:17:27	Host	SRV MEDC01	6.29.14304.0	74.142.71.2	10.0.99.111	
Oct. 5, 2021 15:17:27	Host	SRV RDAPPS01	6.29.14304.0	74.142.71.2	10.0.99.163	
Oct. 5, 2021 15:17:27	Host	SRV MAIL11	6.29.14304.0	74.142.71.4	10.0.99.157	
Oct. 5, 2021 15:17:27	Host	SRV MONITOR02	6.29.14304.0	74.142.71.2	10.0.99.153	
Oct. 5, 2021 15:17:27	Host	TMGFS01	6.29.14304.0	74.142.71.2	10.0.99.165	
Oct. 5, 2021 15:17:27	Host	SRV VM31	6.29.14304.0	74.142.71.2	169.254.2.169	
Oct. 5, 2021 15:17:27	Host	SRV VM30	6.29.14304.0	74.142.71.2	169.254.3.90	
Oct. 5, 2021 15:17:27	Host	SRV MDEC DS01	6.29.14304.0	74.142.71.2	10.0.99.112	
Oct. 5, 2021 15:17:27	Host	SRV VM32	6.29.14304.0	74.142.71.2	169.254.4.228	

ENDPOINT Detection & Response

General Information

ENDPOINT Detection & Response

General Information

- First coined in July 2013 to describe new and more advanced endpoint products by Anton Chuvakin.

ENDPOINT Detection & Response

General Information

- First coined in July 2013 to describe new and more advanced endpoint products by Anton Chuvakin.
- Emphasis is on having visibility and the ability to respond to threats.

ENDPOINT Detection & Response

General Information

- First coined in July 2013 to describe new and more advanced endpoint products by Anton Chuvakin.
- Emphasis is on having visibility and the ability to respond to threats.
- **NOT** a replacement for AntiVirus

ENDPOINT Detection & Response

General Information

- First coined in July 2013 to describe new and more advanced endpoint products by Anton Chuvakin.
- Emphasis is on having visibility and the ability to respond to threats.
- NOT a replacement for AntiVirus
- Often bundled with sister products

ENDPOINT Detection & Response

Yeah... but what does it do?

ENDPOINT Detection & Response

Yeah... but what does it do?

- Gathers activity data from the client computers.

ENDPOINT Detection & Response

Yeah... but what does it do?

- Gathers activity data from the client computers.
- Provides some analysis to look for suspicious activity.

ENDPOINT Detection & Response

Yeah... but what does it do?

- Gathers activity data from the client computers.
- Provides some analysis to look for suspicious activity.
- Give you the ability to investigate and mitigate any issues.

ENDPOINT Detection & Response

Yeah... but what does it do?

- Gathers activity data from the client computers.
- Provides some analysis to look for suspicious activity.
- Give you the ability to investigate and mitigate any issues.
- Some vendors offer monitoring services.

ENDPOINT Detection & Response

Yeah... but what does it do?

- Gathers activity data from the client computers.
- Provides some analysis to look for suspicious activity.
- Give you the ability to investigate and mitigate any issues.
- Some vendors offer monitoring services.
- Is a supplement to the Antivirus product. NOT a replacement.

ENDPOINT Detection & Response

Yeah... but what does it do?

- Gathers activity data from the client computers.
- Provides some analysis to look for suspicious activity.
- Give you the ability to investigate and mitigate any issues.
- Some vendors offer monitoring services.
- Is a supplement to the Antivirus product. NOT a replacement.
- Most EDR vendors offer an AV (next gen AV) product as well.

ENDPOINT Detection & Response

The Traditional Antivirus Experience

ENDPOINT Detection & Response

The Traditional Antivirus Experience

- File matches AV signature and is blocked/quarantined.

ENDPOINT Detection & Response

The Traditional Antivirus Experience

- File matches AV signature and is blocked/quarantined.
- You don't really get a whole lot of information.

ENDPOINT Detection & Response

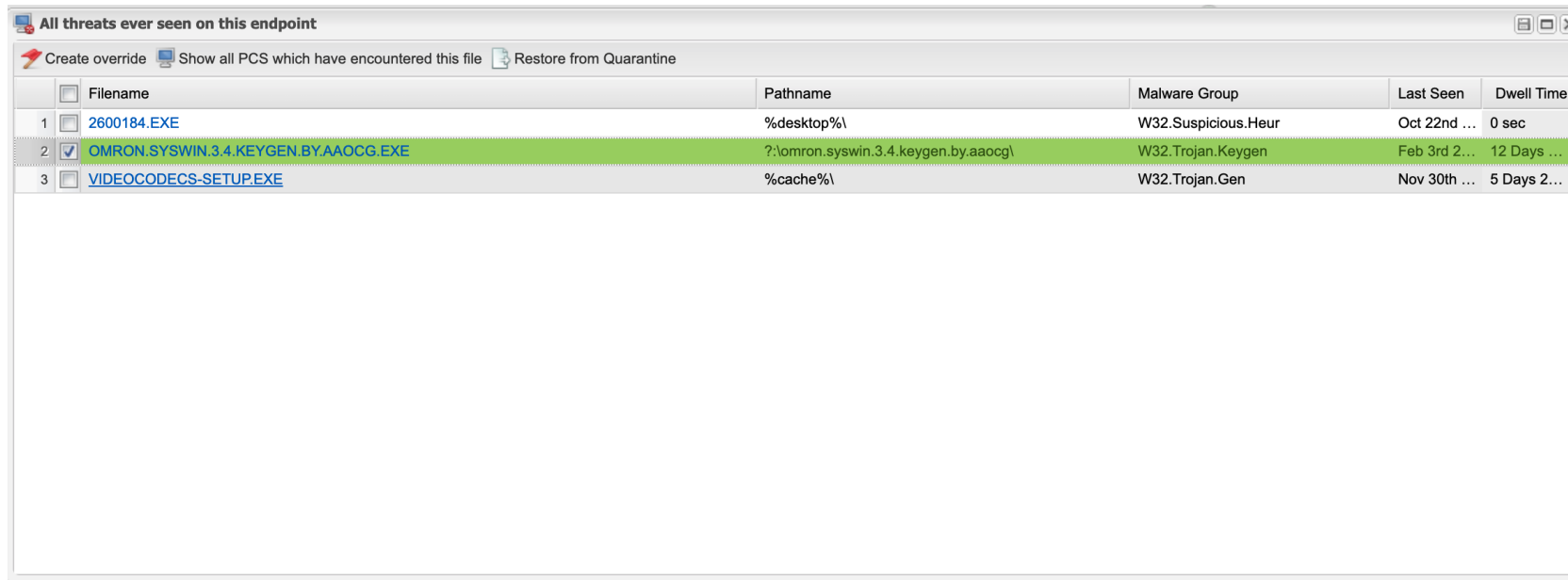
The Traditional Antivirus Experience

- File matches AV signature and is blocked/quarantined.
- You don't really get a whole lot of information.
- AV detection sample:

ENDPOINT Detection & Response

The Traditional Antivirus Experience

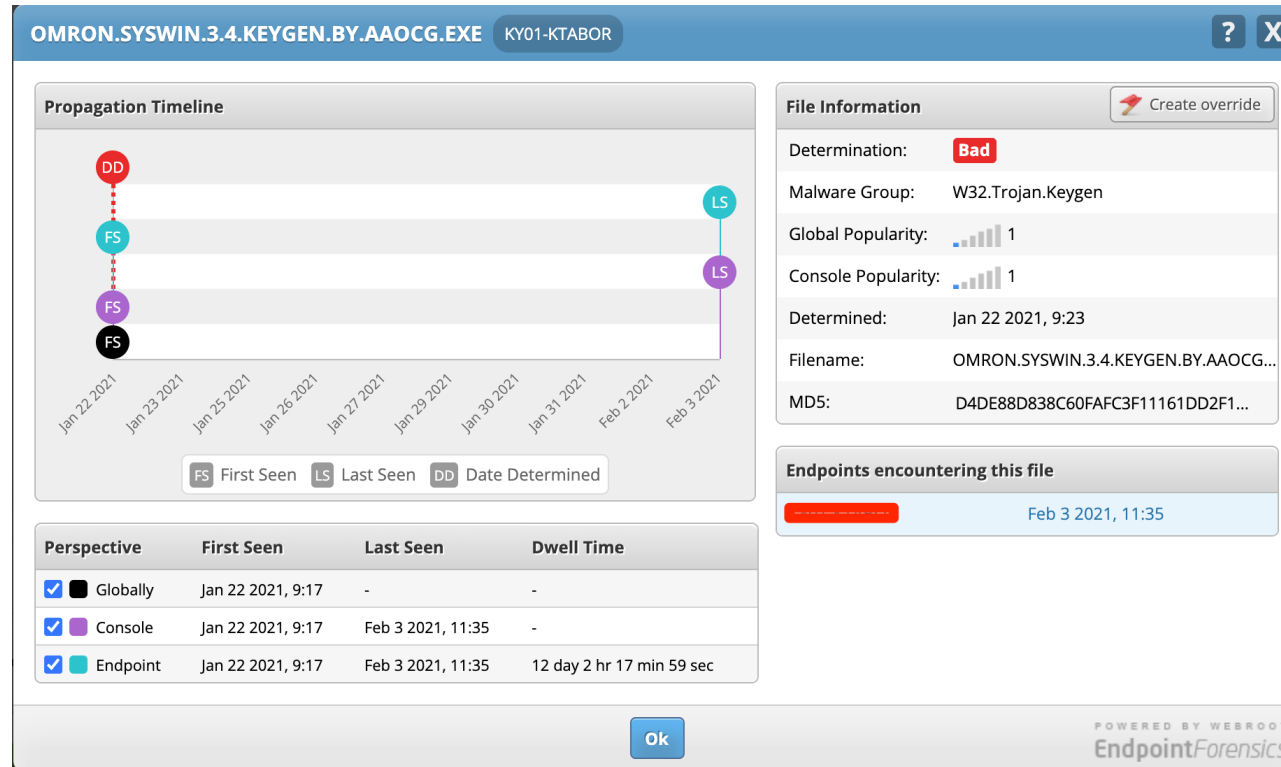
- File matches AV signature and is blocked/quarantined.
- You don't really get a whole lot of information.
- AV detection sample:



	Filename	Pathname	Malware Group	Last Seen	Dwell Time
1	2600184.EXE	%desktop%\	W32.Suspicious.Heur	Oct 22nd ...	0 sec
2	<input checked="" type="checkbox"/> OMRON.SYSWIN.3.4.KEYGEN.BY.AAOCG.EXE	?:\omron.syswin.3.4.keygen.by.aaocg\	W32.Trojan.Keygen	Feb 3rd 2...	12 Days ...
3	VIDEOCODECS-SETUP.EXE	%cache%\	W32.Trojan.Gen	Nov 30th ...	5 Days 2...

ENDPOINT Detection & Response

The Traditional Antivirus Experience



ENDPOINT Detection & Response

The Traditional Antivirus Experience



ENDPOINT Detection & Response

The EDR Experience

WerFault.exe

Unassigned

Closed

Comment

Network contain

Create IOA exclusion

Connect to host

Execution Details

No Machine Learning Exclusions

Comments & Log Entries

File Details

No Quarantined Files

User Details

Host Details

No AV Detections

Network Operations

No Disk Operations

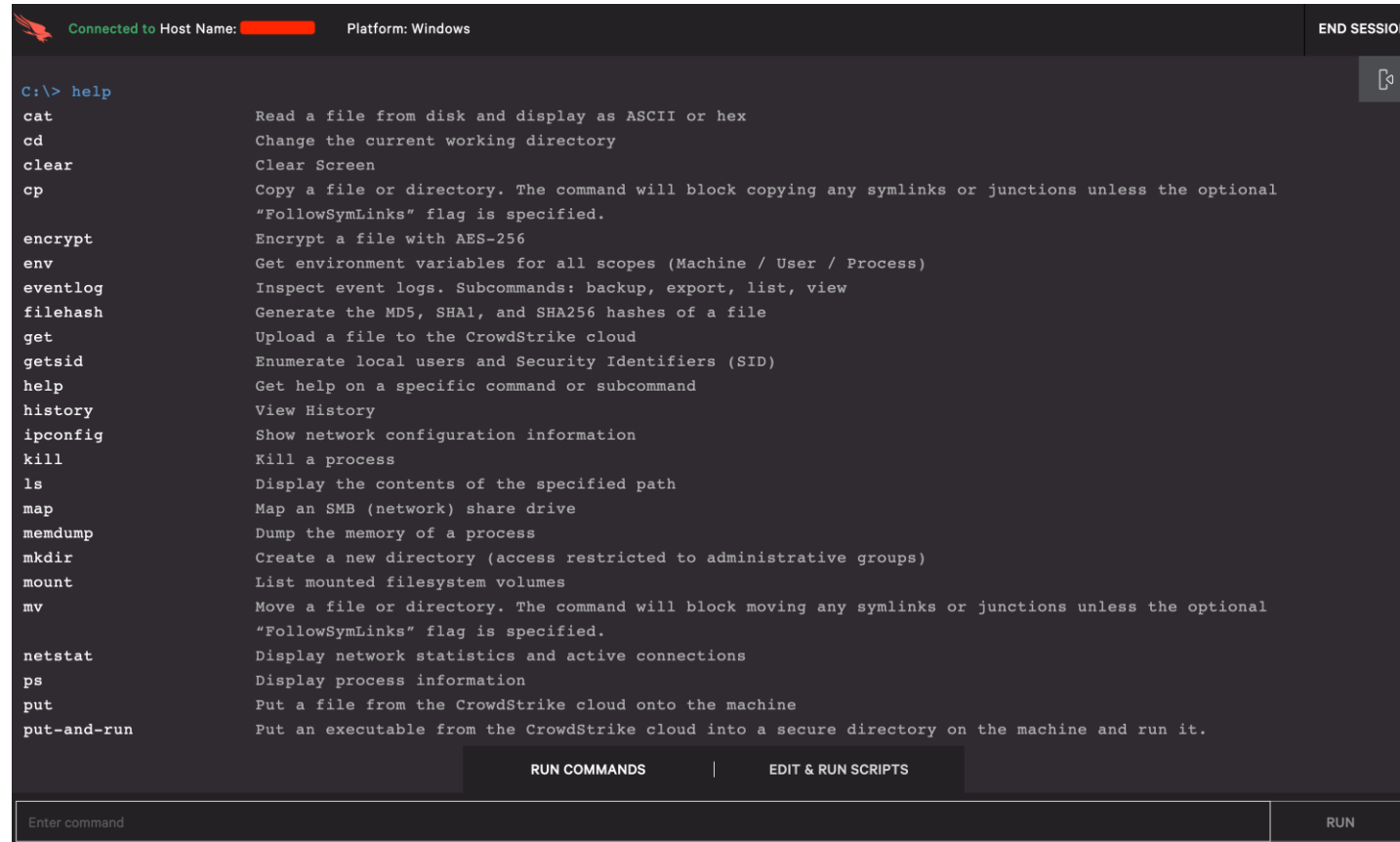
No DNS Requests

No Registry Operations

No Process Operations

ENDPOINT Detection & Response

The EDR Experience



The screenshot displays a terminal window titled "Connected to Host Name: [redacted] Platform: Windows". The terminal shows a list of commands and their descriptions, organized in a table-like format. The commands listed are: cat, cd, clear, cp, encrypt, env, eventlog, filehash, get, getsid, help, history, ipconfig, kill, ls, map, memdump, mkdir, mount, mv, netstat, ps, put, and put-and-run. Each command is followed by a brief description of its function. For example, "cat" is described as "Read a file from disk and display as ASCII or hex". The terminal also includes a "RUN COMMANDS" button and an "EDIT & RUN SCRIPTS" button. At the bottom, there is a text input field labeled "Enter command" and a "RUN" button.

Command	Description
cat	Read a file from disk and display as ASCII or hex
cd	Change the current working directory
clear	Clear Screen
cp	Copy a file or directory. The command will block copying any symlinks or junctions unless the optional "FollowSymLinks" flag is specified.
encrypt	Encrypt a file with AES-256
env	Get environment variables for all scopes (Machine / User / Process)
eventlog	Inspect event logs. Subcommands: backup, export, list, view
filehash	Generate the MD5, SHA1, and SHA256 hashes of a file
get	Upload a file to the CrowdStrike cloud
getsid	Enumerate local users and Security Identifiers (SID)
help	Get help on a specific command or subcommand
history	View History
ipconfig	Show network configuration information
kill	Kill a process
ls	Display the contents of the specified path
map	Map an SMB (network) share drive
memdump	Dump the memory of a process
mkdir	Create a new directory (access restricted to administrative groups)
mount	List mounted filesystem volumes
mv	Move a file or directory. The command will block moving any symlinks or junctions unless the optional "FollowSymLinks" flag is specified.
netstat	Display network statistics and active connections
ps	Display process information
put	Put a file from the CrowdStrike cloud onto the machine
put-and-run	Put an executable from the CrowdStrike cloud into a secure directory on the machine and run it.

ENDPOINT Detection & Response

The EDR Experience

Detections

Q Hash: f13188cdae6d3bdd2a9bc5db677b16e9382f67e5ea32fe9e874 X

2 detections found X





Severity	Tactic	Technique	Time	Status	Triggering file	Assigned to							
Critical	0	Execution	2	Command And Scripti...	2	Last hour	0	New	0	RunNetworkDetective...	2	Unassigned	2
High	2					Last day	0	In Progress	0				
Medium	0					Last week	0	True Positive	0				
Low	0					Last 30 days	2	False Positive	2				
Informational	0					Last 90 days	2	Ignored	0				
+Q	+Q	+Q	+Q	+Q	2 more	+Q	+Q						

☐ Select All

Update & Assign

No grouping

Sort by newest detect time

<input type="checkbox"/>	 High	TACTIC & TECHNIQUE Execution via Command and ...	DETECT TIME Oct. 5, 2021 16:01:12	HOST [REDACTED]	USER NAME [REDACTED]	ASSIGNED TO Unassigned	STATUS False Positi...	
<input type="checkbox"/>	 High	TACTIC & TECHNIQUE Execution via Command and ...	DETECT TIME Oct. 5, 2021 15:49:41	HOST [REDACTED]	USER NAME [REDACTED]	ASSIGNED TO Unassigned	STATUS False Positi...	

ENDPOINT Detection & Response

The EDR Experience

Score - Medium

4.2₁₀

at 2021-10-05T19:49:41Z

Lateral movement event search

Incident event search

Share incident

Description

Objectives in this incident: Gain Access, Follow Through.
Techniques: OS Credential Dumping, Bypass User Account Control, Command and Scripting Interpreter.
Involved hosts and end users: [REDACTED]

Details

Total detections

2

Start time

Oct. 5, 2021 15:17:27

End time

Oct. 5, 2021 16:56:14

Duration

1h 38m 47s

Status

Closed

Tags

Lateral Movement

Network contain all hosts

Host

SRV-DIR10

See more in Host Management

OS	IP Address	Local IP Address	Host ID	Sensor version	Containment status
Windows Server 2016	[REDACTED]	[REDACTED]	9889e046ca314414ab...	6.29.14304.0	Normal

Lateral movement hosts

Hostname	OS	External IP address	Local IP address	Host ID	Sensor version	Network status
[REDACTED]	Windows Server 2...	[REDACTED]	[REDACTED]	c16a9b09733c42c...	6.29.14304.0	Normal
[REDACTED]	Windows Server 2...	[REDACTED]	[REDACTED]	57361b4aa1064d9...	6.29.14304.0	Normal
[REDACTED]	Windows Server 2...	[REDACTED]	[REDACTED]	b4624ee17ad6415...	6.29.14304.0	Normal
[REDACTED]	Windows Server 2...	[REDACTED]	[REDACTED]	73ec786c22554af...	6.29.14304.0	Normal
[REDACTED]	Windows Server 2...	[REDACTED]	[REDACTED]	89c2641047cf491...	6.29.14304.0	Normal
[REDACTED]	Windows Server 2...	[REDACTED]	[REDACTED]	b952f19c52b24c4...	6.29.14304.0	Normal
[REDACTED]	Windows 11	[REDACTED]	[REDACTED]	82f895478083481...	6.29.14304.0	Normal

ENDPOINT Detection & Response

The EDR picture so far...

ENDPOINT Detection & Response

The EDR picture so far...



ENDPOINT Detection & Response

The issues with EDR

ENDPOINT Detection & Response

The issues with EDR

- Too much information

ENDPOINT Detection & Response

The issues with EDR

- Too much information (vendors are happy to offer additional services)

ENDPOINT Detection & Response

The issues with EDR

- Too much information (vendors are happy to offer additional services).
- Beware of false positives and too many alerts.

ENDPOINT Detection & Response

The issues with EDR

- Too much information (vendors are happy to offer additional services).
- Beware of false positives and too many alerts.
- Finally:

ENDPOINT Detection & Response

The issues with EDR

- Too much information (vendors are happy to offer additional services).
- Beware of false positives and too many alerts.
- Finally:



NETWORK Detection & Response

Networks need love too

NETWORK Detection & Response

Networks need love too

- Originates from network-based intrusion detection systems.

NETWORK Detection & Response

Networks need love too

- Originates from network-based intrusion detection systems.



NETWORK Detection & Response

Networks need love too

- Originates from network-based intrusion detection systems.



- Seeks to provide the same level visibility and real time capabilities as EDR

NETWORK Detection & Response

How does it work?

NETWORK Detection & Response

How does it work?

- Dedicated appliances (virtual or physical) in tandem with SPAN ports.

NETWORK Detection & Response

How does it work?

- Dedicated appliances (virtual or physical) in tandem with SPAN ports.
- Appliances analyze network traffic to map the network and build profiles.

NETWORK Detection & Response

How does it work?

- Dedicated appliances (virtual or physical) in tandem with SPAN ports.
- Appliances analyze network traffic to map the network and build profiles.
- The service looks for anomalous behavior or known bad traffic patterns.

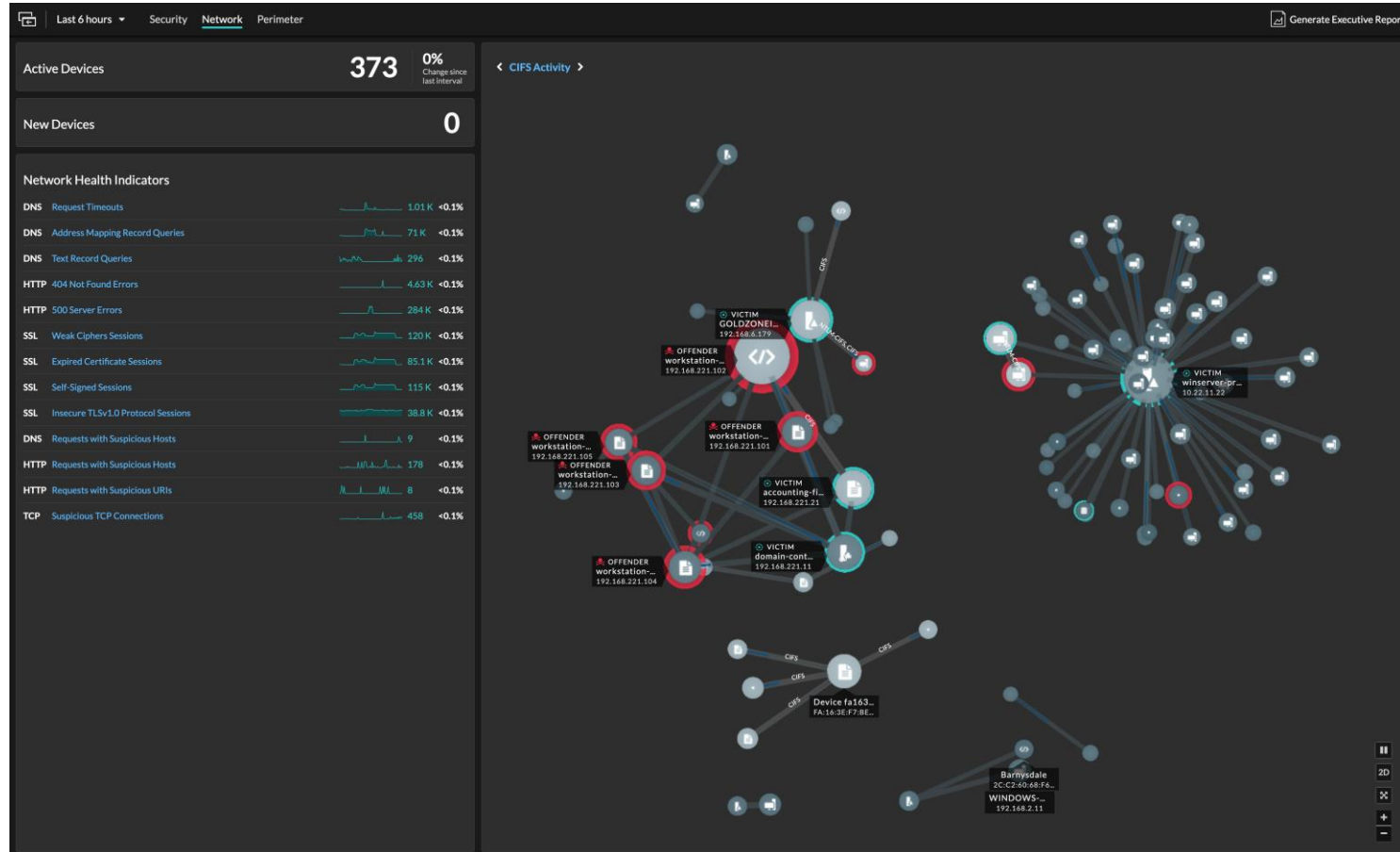
NETWORK Detection & Response

How does it work?

- Dedicated appliances (virtual or physical) in tandem with SPAN ports.
- Appliances analyze network traffic to map the network and build profiles.
- The service looks for anomalous behavior or known bad traffic patterns.
- Threats are met with alerts and can mitigate threats through API connections or other measures. NDR is mostly agentless.

NETWORK Detection & Response

How does it work?



How does it work?



NETWORK Detection & Response

How does it work?



NETWORK Detection & Response

The Skinny

NETWORK Detection & Response

The Skinny

- PRO: Able to capture all network activity for analysis.

NETWORK Detection & Response

The Skinny

- PRO: Able to capture all network activity for analysis.
- CON: You must have the infrastructure to support this functionality.

NETWORK Detection & Response

The Skinny

- PRO: Able to capture all network activity for analysis.
- CON: You must have the infrastructure to support this functionality.
- PRO: Benefit of network health monitoring.

NETWORK Detection & Response

The Skinny

- PRO: Able to capture all network activity for analysis.
- CON: You must have the infrastructure to support this functionality.
- PRO: Benefit of network health monitoring.
- CON: There is a A LOT of data to keep track of.

NETWORK Detection & Response

The Skinny

- PRO: Able to capture all network activity for analysis.
- CON: You must have the infrastructure to support this functionality.
- PRO: Benefit of network health monitoring.
- CON: There is a A LOT of data to keep track of.
- **PRO: Usually offers a lot of integration with other solutions.**

NETWORK Detection & Response

The Skinny

- PRO: Able to capture all network activity for analysis.
- CON: You must have the infrastructure to support this functionality.
- PRO: Benefit of network health monitoring.
- CON: There is a A LOT of data to keep track of.
- PRO: Usually offers a lot of integration with other solutions.
- CON: \$\$\$

NETWORK Detection & Response

The Skinny

- PRO: Able to capture all network activity for analysis.
- CON: You must have the infrastructure to support this functionality.
- PRO: Benefit of network health monitoring.
- CON: There is a A LOT of data to keep track of.
- PRO: Usually offers a lot of integration with other solutions.
- CON: \$\$\$\$ (but not as much as getting compromised)

NETWORK Detection & Response

NDR – Colorized, 2021



EXTENDED Detection & Response (XDR)

Getting into murky waters

EXTENDED Detection & Response (XDR)

Getting into murky waters

- BLUF: There is more to worry about than networks and endpoints <cough, CLOUD, cough>.

EXTENDED Detection & Response (XDR)

Getting into murky waters

- BLUF: There is more to worry about than networks and endpoints <cough, CLOUD, cough>.
- XDR seeks to extend into your cloud & perform an all-in-one detection and response.

EXTENDED Detection & Response (XDR)

Getting into murky waters

- BLUF: There is more to worry about than networks and endpoints <cough, CLOUD, cough>.
- XDR seeks to extend into your cloud & perform an all-in-one detection and response.
- Uses a combination of EDR, NDR, SIEM and API's to perform this.

EXTENDED Detection & Response (XDR)

Getting into murky waters

- BLUF: There is more to worry about than networks and endpoints <cough, CLOUD, cough>.
- XDR seeks to extend into your cloud & perform an all-in-one detection and response.
- Uses a combination of EDR, NDR, SIEM and API's to perform this.
- For Cloud services, will often rely on existing functionality.

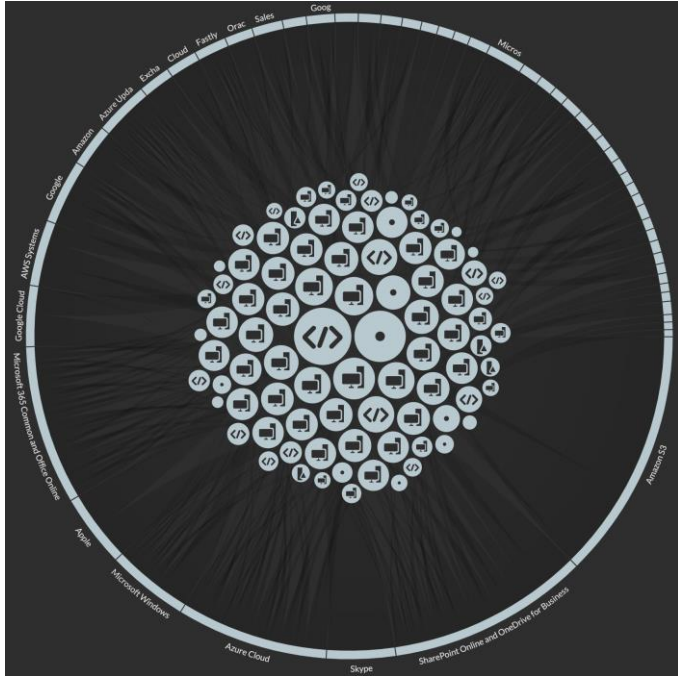
EXTENDED Detection & Response (XDR)

Getting into murky waters

- BLUF: There is more to worry about than networks and endpoints <cough, CLOUD, cough>.
- XDR seeks to extend into your cloud & perform an all-in-one detection and response.
- Uses a combination of EDR, NDR, SIEM and API's to perform this.
- For Cloud services, will often rely on existing functionality.
- You get one stop dashboard to see everything.

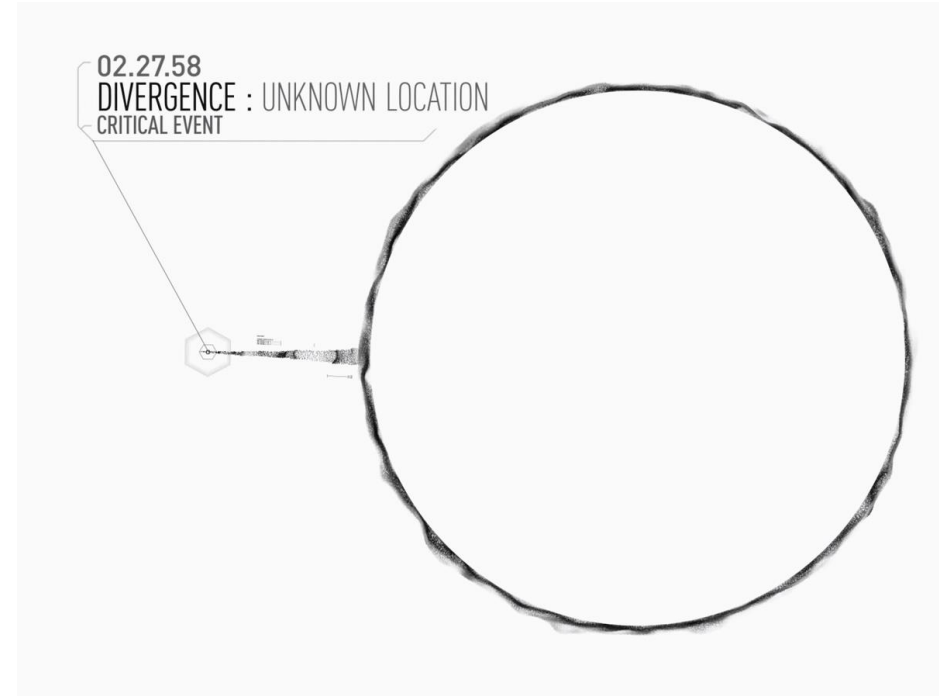
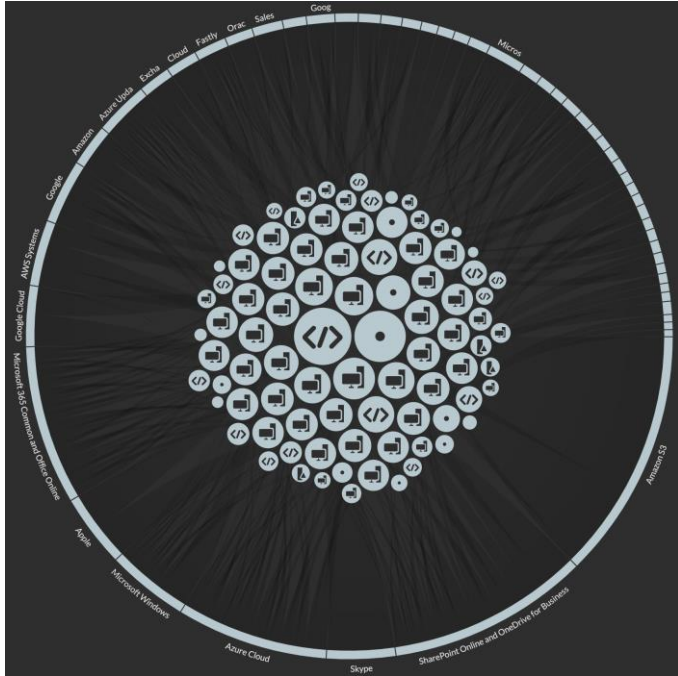
EXTENDED Detection & Response (XDR)

Neat dashboard...



EXTENDED Detection & Response (XDR)

Neat dashboard... Reminds me of the evil AI in “Westworld.”



EXTENDED Detection & Response (XDR)

Summary

EXTENDED Detection & Response (XDR)

Summary

- Combines the best of EDR & NDR.

EXTENDED Detection & Response (XDR)

Summary

- Combines the best of EDR & NDR.
- Adds cloud applications to the mix.

EXTENDED Detection & Response (XDR)

Summary

- Combines the best of EDR & NDR.
- Adds cloud applications to the mix.
- Single pane of glass for everything.

EXTENDED Detection & Response (XDR)

Summary

- Combines the best of EDR & NDR.
- Adds cloud applications to the mix.
- Single pane of glass for everything.
- A LOT of data

EXTENDED Detection & Response (XDR)

Summary

- Combines the best of EDR & NDR.
- Adds cloud applications to the mix.
- Single pane of glass for everything.
- A LOT of data
- A lot to...

MANAGED Detection & Response (MDR)

Summary

MANAGE

MANAGED Detection & Response (MDR)

The murkiest of waters...

MANAGED Detection & Response (MDR)

The murkiest of waters...

- Basically, you are paying the vendor's SOC to babysit the platform.

MANAGED Detection & Response (MDR)

The murkiest of waters...

- Basically, you are paying the vendor's SOC to babysit the platform.
- Keeping track of your E/N/XDR can easily be a full-time job.

MANAGED Detection & Response (MDR)

The murkiest of waters...

- Basically, you are paying the vendor's SOC to babysit the platform.
- Keeping track of your E/N/XDR can easily be a full-time job.
- There is some overlap with various “threat hunting” services.

MANAGED Detection & Response (MDR)

The murkiest of waters...

- Basically, you are paying the vendor's SOC to babysit the platform.
- Keeping track of your E/N/XDR can easily be a full-time job.
- There is some overlap with various “threat hunting” services.
- There is not a lot of consistency in the experience offered by providers.

MANAGED Detection & Response (MDR)

The murkiest of waters...

- Basically, you are paying the vendor's SOC to babysit the platform.
- Keeping track of your E/N/XDR can easily be a full-time job.
- There is some overlap with various “threat hunting” services.
- There is not a lot of consistency in the experience offered by providers.
- Many times, the vendor is reselling other products and managing them on the backend.

Shopping E/N/X/MDR Services

Things to consider

Shopping E/N/X/MDR Services

Things to consider with EDR

- How are threats assessed? Machine learning vs. event limits.

Shopping E/N/X/MDR Services

Things to consider with EDR

- How are threats assessed? Machine learning vs. event limits.
- How many false positives are produced?

Shopping E/N/X/MDR Services

Things to consider with EDR

- How are threats assessed? Machine learning vs. event limits.
- How many false positives are produced?
- How are detections handled?

Shopping E/N/X/MDR Services

Things to consider with NDR

Shopping E/N/X/MDR Services

Things to consider with NDR

- What are the bandwidth capabilities of the appliance?

Shopping E/N/X/MDR Services

Things to consider with NDR

- What are the bandwidth capabilities of the appliance?
- What is the pricing model?

Shopping E/N/X/MDR Services

Things to consider with NDR

- What are the bandwidth capabilities of the appliance?
- What is the pricing model?
- How are potential breaches handled?

Shopping E/N/X/MDR Services

Things to consider with NDR

- What are the bandwidth capabilities of the appliance?
- What is the pricing model?
- How are potential breaches handled?
- How many false positives can you expect?

Shopping E/N/X/MDR Services

Things to consider with NDR

- What are the bandwidth capabilities of the appliance?
- What is the pricing model?
- How are potential breaches handled?
- How many false positives can you expect?
- How many appliances will be required?

Shopping E/N/X/MDR Services

Things to consider with NDR

- What are the bandwidth capabilities of the appliance?
- What is the pricing model?
- How are potential breaches handled?
- How many false positives can you expect?
- How many appliances will be required?
- Will agents be required?

Shopping E/N/X/MDR Services

Things to consider with XDR

Shopping E/N/X/MDR Services

Things to consider with XDR

- All the considerations for EDR & NDR

Shopping E/N/X/MDR Services

Things to consider with XDR

- All the considerations for EDR & NDR
- What cloud services are monitored?

Shopping E/N/X/MDR Services

Things to consider with MDR

Shopping E/N/X/MDR Services

Things to consider with MDR

- What will they do or NOT do?

Shopping E/N/X/MDR Services

Things to consider with MDR

- What will they do or NOT do?
- How will they contact you?

Shopping E/N/X/MDR Services

Things to consider with MDR

- What will they do or NOT do?
- How will they contact you?
- How much visibility will you have?

Shopping E/N/X/MDR Services

Things to consider with MDR

- What will they do or NOT do?
- How will they contact you?
- How much visibility will you have?
- Do they rely on you purchasing third party products?

Shopping E/N/X/MDR Services

Things to consider with MDR

- What will they do or NOT do?
- How will they contact you?
- How much visibility will you have?
- Do they rely on you purchasing third party products?
- All the considerations of EDR, NDR & XDR

I hope you enjoyed BOOOOOOOOOOOMUG

www.Mirazon.com